RECEIVED
CENTRAL FAX CENTER

JAN 3 0 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Leung et al.**

Serial No.: **09/738,243**

Filed: **December 15, 2000**

For: **Method and Apparatus for Dual Hardware and Software Cryptography**

§ Group Art Unit: **2136**

§

§ Examiner: **Colin, Carl G.**

§

§ Attorney Docket No.: **AUS920000814US1**

§

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on January 30, 2006.

By: Kim Gault
Kim Gault

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37)

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEY FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER

JAN 3 0 2006

Yee & Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Carl G. Colin** **Group Art Unit 2136**	Facsimile No.: **571/273-8300**
From: Kim Gault Legal Assistant to Wayne Bailey	No. of Pages Including Cover Sheet: **25**

Message:

Enclosed herewith:

- Transmittal Document; and
- Appeal Brief.

Re: Application No. **09/738,243**
Attorney Docket No: **AUS920000814US1**

Date: Monday, January 30, 2006

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	*This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.*

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

RECEIVED
CENTRAL FAX CENTER

JAN 3 0 2006

Docket No. AUS920000814US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Leung et al.**	§	
	§	Group Art Unit: **2136**
Serial No. **09/738,243**	§	
	§	Examiner: **Colin, Carl G.**
Filed: **December 15, 2000**	§	
	§	
For: **Method and Apparatus for Dual Hardware and Software Cryptography**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on January 30, 2006.

By: Kim Gauld
Kim Gauld

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on November 28, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

01/31/2006 CNGUYEN 00000104 090447 09738243
01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation of Armonk, N.Y.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-46

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 5-7, 11, 15-18, 20-25, 30-32, 36, 40-41 and 44-46
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1-4, 8-10, 12-14, 19, 26-29, 33-35, 37-39, and 42-43
4. Claims allowed: none
5. Claims rejected: 1-4, 8-10, 12-14, 19, 26-29, 33-35, 37-39, and 42-43
6. Claims objected to: none

C. CLAIMS ON APPEAL

The claims on appeal are: 1-4, 8-10, 12-14, 19, 26-29, 33-35, 37-39, and 42-43

STATUS OF AMENDMENTS

No amendment after final was filed for this case.

SUMMARY OF CLAIMED SUBJECT MATTER

Cryptography is a technique for keeping information secure, where information is enciphered (scrambled) so that it is difficult to determine the meaning without the appropriate decipher key(s). Cryptographic operations can be performed using either hardware-based or software-based solutions, with the choice of which type of system to use typically being based on various trade-offs such as cost, speed of operation and susceptibility to system compromise or malicious hacking. The present invention is generally directed to a technique for dynamically choosing between a hardware and software-based solution for performing cryptographic operations, with a corresponding key conversion to convert the key to a form suitable for use by the selected hardware or software-based solution.

A. CLAIM 1 - INDEPENDENT

Claim 1 is specifically directed to a method in a data processing system for executing cryptographic operations. Responsive to a request to perform a cryptographic operation, a dynamic selection is made between a software process and a hardware process for performing the cryptographic operation based on a policy. The cryptographic operation, which is the encryption of data using a key, is performed using the dynamically selected process. The key is converted to a form useable by the selected process if the key is in an unusable form by the selected process, where the key is a software key and the selected process is the hardware process and the step of converting the key comprises converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation (Specification page 14, line 11 – page 15, line 12; Figure 4, all blocks).

B. CLAIM 8 - INDEPENDENT

Claim 8 is specifically directed to a method in a data processing system for executing cryptographic operations. Responsive to a request to perform a cryptographic operation, a dynamic selection is made between a software process and a hardware process for performing the cryptographic operation based on a policy. The cryptographic operation, which is the encryption of data using a key, is performed using the dynamically selected process. The key is

a hardware key and is converted into a software form useable by the software process for performing the cryptographic operation (Specification page 14, line 11 – page 15, line 12; Figure 4, all blocks).

C. CLAIM 26 – INDEPENDENT AND MEANS-PLUS-FUNCTION

Claim 26 is a system claim corresponding to method Claim 1, and the summary of Claim 1 is applicable for Claim 26, and thus is hereby incorporated by reference.

Claim 26 is also a means-plus-function claim, and the structure corresponding to each of the recited means-for elements is described at Specification page 6, line 28 – page 9, line 24, and shown by reference character 200 in Figure 2.

D. CLAIM 33 – INDEPENDENT AND MEANS-PLUS-FUNCTION

Claim 33 is a system claim corresponding to method Claim 8, and the summary of Claim 8 is applicable for Claim 33, and thus is hereby incorporated by reference.

Claim 33 is also a means-plus-function claim, and the structure corresponding to each of the recited means-for elements is described at Specification page 6, line 28 – page 9, line 24, and shown by reference character 200 in Figure 2.

E. CLAIM 42 – INDEPENDENT

Claim 42 is a system claim corresponding to method Claim 8, and the summary of Claim 8 is applicable for Claim 42, and thus is hereby incorporated by reference.

F. CLAIM 43 – INDEPENDENT

Claim 43 is a system claim corresponding to method Claim 1, and the summary of Claim 1 is applicable for Claim 43, and thus is hereby incorporated by reference.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1-4, 8-10, 12-14, 19, 26-29, 33-35, 37-39 and 42-43)

Claims 1-4, 8-10, 12-14, 19, 26-29, 33-35, 37-39 and 42-43 stand rejected under 35 U.S.C. § 103 as being unpatentable over US Patent 5,778,072 to Samar in view of US Patent 6,393,565 to Lockhart et al.

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-4, 8-10, 12-14, 19, 26-29, 33-35, 37-39 and 42-43)

Claims 1-4, 8-10, 12-14, 19, 26-29, 33-35, 37-39 and 42-43 stand rejected under 35 U.S.C. § 103 as being unpatentable over US Patent 5,778,072 to Samar in view of US Patent 6,393,565 to Lockhart et al. Appellants show error in such rejection as follows.

A.1. Claims 1-4, 19, 26-29 and 43

With respect to Claim 1, such claim recites the claimed feature of "wherein the key is a software key and the selected process is the hardware process and further comprising converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation". As can be seen, the key that is used for encryption of data is a software key *that is converted to a hardware form* useable by the hardware process for performing cryptographic operations. None of the cited references teach or suggest any type of key conversion at all. For example, the cited Samar reference teaches use of either a smartcard or a software process for performing a cryptographic operation, based upon whether a smartcard is present (Figure 2, blocks 205, 207 and 221). If a smartcard is present, the user is authenticated by initiating a challenge/response protocol, or a particular password/personal identification number protocol, with the user's smartcard (col. 6, lines 6-11; Figure 2, blocks 207 and 135). The smart card will return a value to the operating system indicating whether the authentication was successful (col. 6, lines 17-19). There is no type of key conversion in this process, as *the key is secretly maintained within the smartcard such that it cannot be externally accessed* (col. 6, lines 50-54). If a smartcard is not present in the system, the user is authenticated with any of the selected encryption services 129 (col. 6, lines 36-38). Since in this scenario no smartcard is present, the key store manager requests (from the selected encryption service) a private key for the user. This private key is written to the user information file (col. 6, lines 40-46). In this scenario of no smartcard being present, there also is no type of key conversion of a software key into a hardware form usable by the hardware process, as this scenario describes use of a software key by a software process. Quite simply, there is no teaching or suggestion of converting a

software key into a hardware form useable by a hardware process for performing a cryptographic operation of encrypting data using such converted key.

For the encryption operation described by Samar at col. 7, lines 10-44, the data to be encrypted is passed to the smartcard where it is encrypted using a "non-readably stored key" (col. 7, lines 30-31), *such that the user's private key is never exposed outside the card* (col. 7, lines 37-44). Again, there is no type of key conversion performed, as *the cited Samar reference is keen on maintaining a preexisting hardware encryption key internal to the smartcard, which is not readable or otherwise accessible outside the card* (col. 2, lines 19-27; col. 6, lines 50-54; col. 7, lines 37-44).

The Examiner cites three Samar passages as evidencing the conversion of a software key to a form usable by the hardware encryption process: (1) col. 5, line 65 – col. 5, line 6 (Appellant's note – it is believed this is a typographical error and that the Examiner meant to cite col. 4, line 65 – col. 5, line 6 as the cited passage of col. 5, line 65 – col. 5, line 5 is unclear/confusing); (2) col. 7, lines 32-33; (3) col. 8, lines 30-37; and (4) col. 2, lines 28-35. Appellants will now discuss each of these cited passages individually.

(1) The passage cited at col. 5, line 65 – col. 5, line 6 (again, it is assumed this passage was intended to be col. 4, line 65 – col. 5, line 5) describes operations performed by a key store manager, including processing requests to create public or private key data using an encryption service, writing such key data to a file/storage, obtaining existing private key data from either a smart card or user information file/storage and processing encryption requests. Of critical importance is that this cited passage does not describe, teach or otherwise suggest any type of key conversion process, and thus does not teach or otherwise suggest the claimed feature of "wherein the key is a software key and the selected process is the hardware process and the step of converting the key comprises *converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation*". Rather, Samar's use of a smartcard as a hardware process for performing cryptographic operations uses a preexisting hardware encryption key maintained internal to the smartcard (col. 2, lines 19-27; col. 6, lines 50-54; col. 7, lines 37-44).

(2) The passage cited at col. 7, lines 32-33 contains an obvious typographical error, and the word 'can' should really be 'cannot', and this typographical error is clear when this cited passage is read in context. As can be seen at col. 7, lines 30-31, it states that the smart card encrypts the data using user A's private key which is *non-readably stored* therein. It is clear that storing something non-readably means that it is stored so that it *cannot* be read. This is also clear by the Samar passage at col. 6, lines 50-54, where it states:

> From the foregoing it can be seen that where the user has a smart card 123 **the user's private key is never exposed to the system 100**, and thus cannot be compromised, even if the system 100 is compromised during or after the authentication process.

and at col. 7, lines 37-44 where it states:

> Because the private key operation is performed entirely within the smart card 123, **user A's private key is never exposed to the computer 101, and never resides in the addressable memory 103, the storage device 113, or any other publically available facility**. Thus, even if the system 100 had been previously compromised, or is subsequently compromised, user A's private key would still be secure.

Appellants thus urge that this use of the word 'can' is a typographical error which should instead read as 'cannot' when viewed in the proper context, and thus this passage does not establish any ability to read or otherwise access the smart card's internally maintained key for any type of key conversion operation.

(3) The passage cited at Samar col. 8 describes a *decryption* operation, whereas Claim 1 is directed to an *encryption* operation, and thus these teachings are not germane to

any type of claimed *encryption* elements. In any event, this passage does not describe any type of key conversion being performed as a part of an encryption process.

(4) The passage cited at Samar col. 2 does not teach or otherwise suggest any type of key conversion, and thus does not teach or otherwise suggest the specific claimed feature of "wherein the key is a software key and the selected process is the hardware process and the step of converting the key comprises *converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation*".

The Examiner appears to acknowledge such teaching/suggestion deficiency, by stating:

> "The use of Lockhart in the rejection is to fully support *the key conversion already disclosed by Samar*. Examiner respectfully asserts that Samar *either alone or in combination with Lockhart* discloses the amended claimed limitations." (emphasis added by Appellants)

Appellants urge that this 'hedge' statement is evidence unto itself that the Examiner is not themself certain that Samar teaches any type of key conversion, and as shown above Samar does not disclose any type of key conversion of a software key into a hardware form useable by the hardware process for encrypting data. Appellants will now show that the cited Lockhart reference does not overcome such teaching/suggestion deficiency.

Lockhart describes a smart card having a limited history file that can only maintain a limited number of historic or old keys. Accordingly, when a new key is received and needs to be saved in the smart card, the oldest history key is stored in a separate overflow memory such that the newly received key can be saved in the smartcard (col. 4, lines 2-13). There is no description of any type of key conversion of a software key into a hardware form useable by the hardware process for encrypting data. The only described functions performed on the actual key itself are generating a new key, sending a key, receiving a key and storing a key (col. 3, line 54 – col. 4, line 13 and col. 4, line 46 – col. 5, line 3).

The cited Lockhart reference also describes the decrypting of newly received encrypted keys, and the encrypting of old keys for archival storage (col. 4, line 46 – col. 5, line 12). Such encryption and decryption of keys does not teach or otherwise suggest the claimed feature of "wherein the key is a software key and the selected process is the hardware process and the step of converting the key comprises *converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation*" as expressly recited in Claim 1. Rather, this encryption of a key is done as a precursor step to archiving the key.

Nor does the cited Lockhart reference teach any conditional operation being performed based upon whether the key is in an unusable form by the selected process. Claim 1 expressly recites a step of "converting the key to a form useable by the selected process *if the key is in an unusable form by the selected process*" (emphasis added), the selected process being a hardware process. Lockhart's smartcard merely stores keys, and has no hardware encryption capability (col. 3, lines 8-19; Figure 2, element 102). The cryptographic operations are instead performed by the cryptographic data manager 104 (Figure 3, elements 202, 206, 232 and 234). Importantly, this cited reference only teaches use of a single encryptor 206, so *there would have been no motivation to conditionally convert between different types of encryption keys (hardware and software) based on the type of encryption process being used as there is but a single encryption process*. The fact that a prior art device could be modified so as to produce the claimed device is not a basis for an obviousness rejection unless the prior art suggested the desirability of such a modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). There is simply no suggestion or other motivation to modify the teachings of Lockhart to perform the conditional key conversion step when encrypting data, as described above, and thus Claim 1 is further shown to have been erroneously rejected under 35 U.S.C. 103.

It is thus urged that Claim 1 has been erroneously rejected, as there are missing claimed features not taught or suggested by any of the cited references[1].

[1] To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also. In re Royka*, 490 F.2d 580 (C.C.P.A. 1974). If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

A.2. Claims 8, 10, 12-14, 33, 35, 37-39 and 42

With respect to Claim 8, such claim recites performing the cryptographic operation using the selected process, where the cryptographic operation is an encryption of data using a key, where the key is a hardware key and the selected process is the software process and further comprising converting the hardware key into a software form useable by the software process for performing the cryptographic operation. As described above with respect to Claim 1, the cited Samar reference does not teach any type of key conversion from one form to another, and in fact the reference is keen on not allowing hardware keys to be used with or accessed by other types of cryptographic operations due to security concerns (col. 6, lines 50-54; col. 7, lines 37-44). It is thus urged that Claim 8 is not obvious in view of the cited references, as there are missing claimed features not taught or suggested by any of the cited references.

A.3. Claims 9 and 34

Applicants initially show error in the rejection of Claim 9 (and similarly for Claim 34) for reasons given above with respect to Claim 8 (of which Claim 9 depends upon).

Further with respect to Claim 9 (and similarly for Claim 34), such claim further defines the policy which is used to determine which process (hardware or software) is to be used for performing the encryption of data, and is specifically directed to a policy that comprises a set of rules used to *minimized available resources consumed in performing the cryptographic operation*. In rejecting Claim 9, the Examiner states that such claimed feature is taught by Samar at col. 3, line 45 – col. 4, line 7. Appellants urge that this cited passage describes various features of the Samar invention, including (1) logging out a user's session if they remove the smart card (col. 3, lines 45-52), (2) use of existing applications to take advantage of either the smart card or host encryption services (col. 3, lines 53-62), and (3) an ability to choose between use of the smart card or host encryption services based upon the type of user using the system (col. 3, line 63 – col. 4, line 7). While item (3) does mention criteria that is used to determine which of the smart card or host encryption services to use, such passage does not teach or otherwise suggest *a set of rules that is used to minimize available resources* that are consumed in performing the cryptographic operation. Rather, this cited passage merely states that the choice is made based on the *type of user*. Thus, the Examiner has failed to establish a prima facie

showing of obviousness with respect to Claim 9, and accordingly the burden has not shifted to Applicant to rebut such improper obviousness assertion[2]. In addition, as a prima facie case of obviousness has not been established with respect to Claim 9, such claim has thus been erroneously rejected[3].

In conclusion, Appellants have shown error in the final rejection of all pending claims, and respectfully requests that the Board reverse such final rejection.

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

[2] In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. *Id.*
[3] *In re Fine, supra.*

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method in a data processing system for executing cryptographic operations, the method comprising:

responsive to a request to perform a cryptographic operation, dynamically selecting between one of a software process and a hardware process within the data processing system for performing the cryptographic operation based on a policy, to form a selected process; and

performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, and wherein the step of performing the cryptographic operation includes converting the key to a form useable by the selected process if the key is in an unusable form by the selected process, wherein the key is a software key and the selected process is the hardware process and the step of converting the key comprises converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation.

2. The method of claim 1, wherein the policy includes selecting the one based on available resources to perform the cryptographic operation.

3. The method of claim 1, wherein the policy includes selecting the one resulting in a fastest completion of the cryptographic operation.

4. The method of claim 1, wherein the selecting step includes:

selecting the one using a preference associated with the request.

8. A method in a data processing system for executing cryptographic operations, the method comprising:

responsive to a request to perform a cryptographic operation, dynamically selecting between one of a software process and a hardware process within the data processing system for performing the cryptographic operation based on a policy, to form a selected process; and

performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, wherein the key is a hardware key and the selected process is the software process and further comprising:

converting the hardware key into a software form useable by the software process for performing the cryptographic operation.

9. The method of claim 8, wherein the policy comprises a set of rules used to minimize available resources consumed in performing the cryptographic operation.

10. The method of claim 8, wherein the policy comprises a set of rules used to maximize a speed at which the cryptographic operation is performed.

12. The method of claim 8, wherein the cryptographic operation is one of a message digest and a public-private key encryption.

13. The method of claim 8, wherein the request is received from an application.

14. The method of claim 13, wherein the request is received from the application using an application program interface call made by the application.

19. The method of claim 2, wherein the available resources include available processing resources and memory.

26. A data processing system for executing cryptographic operations, the data processing system comprising:

selecting means for dynamically selecting between one of a software process and a hardware process within the data processing system for performing a cryptographic operation based on a policy, to form a selected process in response to a request to perform the cryptographic operation; and

performing means for performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, and wherein the performing means includes converting means for converting the key to a form useable by the selected process if the key is in an unusable form by the selected process, wherein the key is a software key and the selected process is the hardware process and the converting means comprises means for converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation.

27. The data processing system of claim 26, wherein the policy includes selecting the one based on available resources to perform the cryptographic operation.

28. The data processing system of claim 26, wherein the policy includes selecting the one resulting in a fastest completion of the cryptographic operation.

29. The data processing system of claim 26, wherein the selecting means includes:

selecting means for selecting the one using a preference associated with the request.

33. A data processing system for executing cryptographic operations, the data processing system comprising:

selecting means for dynamically selecting between one of a software process and a hardware process within the data processing system for performing a cryptographic operation based on a policy, to form a selected process in response to a request to perform the cryptographic operation; and

performing means for performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, and wherein the performing means includes converting means for converting the key to a form useable by the selected process if the key is in an unusable form by the selected process, wherein the key is a hardware key and the selected process is the software process and the converting means comprises means for converting the hardware key into a software form useable by the software process for performing the cryptographic operation.

34. The data processing system of claim 33, wherein the policy comprises a set of rules used to minimize available resources consumed in performing the cryptographic operation.

35. The data processing system of claim 33, wherein the policy comprises a set of rules used to maximize a speed at which the cryptographic operation is performed.

37. The data processing system of claim 33, wherein the cryptographic operation is one of a message digest and a public-private key encryption.

38. The data processing system of claim 33, wherein the request is received from an application.

39. The data processing system of claim 38, wherein the request is received from the application using an application program interface call made by the application.

42. A data processing system comprising:

a bus system;

a communications unit connected to the bus, wherein data is sent and received using the communications unit;

a memory connected to the bus system, wherein a set of instructions are located in the memory; and

a processor unit connected to the bus system, wherein the processor unit executes the set of instructions to (i) dynamically select between one of a software process and a hardware

process within the data processing system for performing a cryptographic operation based on a policy, to form a selected process; (ii) perform the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, wherein the key is a hardware key and the selected process is the software process; and (iii) convert the hardware key into a software form useable by the software process for performing the cryptographic operation.

43. A data processing system comprising:

a bus system;

a communications unit connected to the bus, wherein data is sent and received using the communications unit;

a memory connected to the bus system, wherein a set of instructions are located in the memory; and

a processor unit connected to the bus system, wherein the processor unit executes the set of instructions to (i) dynamically select between one of a software process and a hardware process within the data processing system for performing a cryptographic operation based on a policy, to form a selected process; (ii) perform the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, wherein the key is a software key and the selected process is the hardware process; and (iii) convert the software key into a hardware form useable by the hardware process for performing the cryptographic operation.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.